

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

BRUCE SINGER,

Defendant.

Criminal No. 17-30007-MGM

MEMORANDUM & ORDER REGARDING MOTIONS TO SUPPRESS

(Dkt. Nos. 60 & 62)

December 12, 2018

MASTROIANNI, U.S.D.J.

Defendant Bruce Singer has been charged with seven counts related to the possession, distribution, and receipt of child pornography. He moved to suppress evidence seized from his home (Dkt. No. 60) and evidence found on his laptop (Dkt. No. 62). For the reasons set forth below, both motions will be denied.

I. FACTUAL BACKGROUND

There are two warrants at issue: a warrant to search Defendant's house and a warrant to search his laptop. Detective Sergeant Mark Popielarczyk of the Easthampton Police Department sought and obtained the warrant for Defendant's house. (Dkt. No. 70.) As explained in Detective Sergeant Popielarczyk's affidavit, the Massachusetts State Police Internet Crimes Against Children Task Force got a tip there was child pornography posted on a Facebook account belonging to someone living in Easthampton. (*Id.* at 2-3.) A warrant was executed at that person's address, which revealed the person was communicating with others about, and sharing or trading, child pornography. (*Id.* at 3-4.) One of the others had a Hotmail email address. (*Id.*) Through an administrative subpoena, police obtained an IP address and an alternate email address (consisting of Defendant's first initial and last name) associated with the Hotmail account. (*Id.* at 4.) An additional

subpoena revealed that Defendant was the subscriber for the IP address and provided Defendant's home address. (*Id.* at 5.) A Registry of Motor Vehicles query confirmed Defendant resides at that address. (*Id.* at 7.)

Detective Sergeant Popielarczyk, based on his training and experience, described common behaviors of people who collect and trade child pornography. (*Id.* at 8-10.) In particular, he explained that sexually explicit depictions of children tend to be important to such individuals; these individuals are unlikely to destroy a collection of child pornography; sexually explicit depictions of children can be found on a variety of media, including videotapes, photographs, and digital images or videos stored on electronic devices and removable media; and these media have been found in people's homes, motor vehicles, and on their persons. (*Id.* at 8-9.) Searches of residences reveal evidence showing ownership or use of digital media and internet service accounts, as well as dominion and control of the residences searched. (*Id.* at 9-10.)

The warrant authorized officers to search Defendant's house for "Any and all computers, 'smart phones,' 'mobile data devices' and 'network' equipment systems," which were explained in more detail in Addendum A to the warrant application. (Dkt. No. 60-1.) Addendum A is a non-exhaustive list of computers and other devices on which digital media can be stored, as well as input devices, output devices, computer system documentation, data files, and other files, records, logs, and materials. (*Id.*)

The warrant was executed on June 25, 2015. Officers seized certain technology from Defendant's home, including two iPhones; two other cell phones; a Nook tablet; DVDs, CDs, VHS tapes, and cassette tapes; two recorders with tapes; approximately 15 digital storage devices, including hard drives, USB drives, and memory cards; and CDs containing samples of evidence, including images from a laptop and previews of the contents of two hard drives.

The day before the warrant was executed, Defendant asked a neighbor to fix his laptop; Defendant left the laptop with the neighbor. The neighbor learned about Defendant's arrest and the search of his home. The neighbor did not repair Defendant's laptop and instead contacted the police to turn over the laptop. Massachusetts State Trooper Gary Hebert retrieved it from the neighbor and applied for and obtained a warrant to search the laptop.

That warrant application contained information from Detective Sergeant Popielarczyk's affidavit, as well as information about the evidence seized from Defendant's home. (Dkt. No. 75 at 3-7.) In particular, Trooper Hebert assisted in the search of Defendant's home, during which he personally observed sexually explicit images of children found on various electronic devices (including computers, a cell phone, a tablet, and a hard drive). (*Id.* at 7.) Police seized more than 10,000 explicit images from Defendant's house. (*Id.*) Trooper Hebert's affidavit also included a list of items to be seized from the laptop, including files, data, or information regarding (1) access, possession, control, use, and/or ownership of the laptop; (2) the laptop's systems configuration; (3) "internet history, user accounts, correspondence, etc."; (4) access, possession, control, use, and/or ownership of any evidence found on the laptop; and (5) directories, sub-directories, file names, and dates and times of file creation, modification, deletion, and/or access. (*Id.* at 3.)

Defendant moved to suppress all evidence seized from his home and laptop on the ground that both warrants are overbroad.

II. ANALYSIS

The analyses for both suppression motions are analogous. The court begins with the issue of probable cause and then addresses whether either warrant is overbroad.

A. The Warrants Are Supported by Probable Cause.

"A warrant application must demonstrate probable cause to believe that (1) a crime has been committed—the "commission" element, and (2) enumerated evidence of the offense will be

found at the place searched—the so-called “nexus” element.” *United States v. Dixon*, 787 F.3d 55, 59 (1st Cir. 2015) (quoting *United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999)). The “inquiry is a practical, common-sense one that takes into account the totality of the circumstances.” *Dixon*, 787 F.3d at 59 (internal quotation marks and citations omitted). “[T]he facts presented to the [judge approving the warrant] need only ‘warrant a man of reasonable caution’ to believe that evidence of a crime will be found.” *Feliz*, 182 F.3d at 86 (quoting *Texas v. Brown*, 460 U.S. 730, 742 (1983) (plurality opinion)).

Both warrants are supported by probable cause that evidence of Defendant’s possession and/or dissemination of child pornography would be found in his house and on his laptop. The warrant for the house was based on a tip about child pornography on a Facebook account; evidence seized from the Facebook account owner’s home, including communications with an email address sharing child pornography; and information obtained from administrative subpoenas revealed the email address was Defendant’s and provided his home address. This is a sufficient showing that there was probable cause to believe evidence of child pornography existed in Defendant’s house.

The warrant for the laptop was based on the same evidence as the warrant for the house plus additional child pornography-related evidence seized from the house before police knew about and recovered the laptop. As a result, the warrant for the laptop is also supported by probable cause.

B. The Warrants Are Not Overbroad.

Defendant argues both warrants are overbroad because the house warrant described virtually every electronically-stored item in Defendant’s home, the laptop warrant gave “nearly unrestricted access” to the contents of his laptop, and neither warrant contains limits for items not included in the warrant. (Dkt. No. 61 at 3; Dkt. No. 63 at 3.)

When considering whether a warrant is overbroad, “the circumstances and nature of the activity under investigation dictate the specificity with which a warrant may be drawn”; “thus

[courts] have held that “[t]he proper metric . . . is whether it was reasonable to provide a more specific description of the items at that juncture of the investigation.” *United States v. Kuc*, No. 11-10014-DPW, 2012 WL 2244796, at *4 (D. Mass. June 14, 2012) (citation omitted).

1. House Warrant

A warrant for the search and seizure of computers and digital storage media is not overbroad or unreasonable if there is probable cause establishing “sufficient chance of finding some needles in the computer haystack.” *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999). Similarly, the Ninth Circuit has held that a warrant for electronic storage devices in a defendant’s possession is not overbroad if the government has evidence that the defendant received child pornography but does not know where it is stored. *See United States v. Ivers*, 430 F. App’x 573, 575 (9th Cir. 2011) (“The FBI could not have provided a more specific description of the items sought because . . . the government knew that [defendant] had received pornographic images ‘but had no way of knowing where the images were stored.’” (citation omitted)).

The analysis in this case is similar to that in *United States v. Burdulis*, No. 10-40003-FDS, 2011 WL 1898941 (D. Mass. May 19, 2011). The warrant in *Burdulis* authorized the seizure of “[a]ll objects capable of storing digital data of any form.” *Id.* at *4. It allowed “officers to search defendant’s home and seize, among other things, central processing units, digital cameras, thumb drives, floppy disks, compact disks, and digital video disks (DVDs),” as well as “user’s manuals, computer access codes, and evidence of control, use or ownership.” *Id.* The defendant in that case, like Defendant here, argued the warrant was overbroad. *Id.* And here, as in *Burdulis*, Defendant has not established that the warrant was impermissibly broad by “allow[ing] the seizure of information for people unrelated to the probable cause in the warrant, [having been] issued in reliance on misinformation regarding the need for immediate seizure, or [having been] executed in breach of the protocols specified in the warrant.” *Id.* at *5.

As the *Burdulis* court explained,

[w]hen seizing a defendant's home computer systems, there is simply no way to be sure exactly what an electronic file contains without somehow examining its contents. If there was probable cause to believe that evidence of [child pornography] would be found on defendant's home computer systems, a warrant authorizing the government to seize all of defendant's home computer systems and digital storage media was not overbroad.

Id. (internal quotation marks and citation omitted). The court continued:

Defendant also points to no authority requiring the government to abstain from seizing his home computer systems and storage media simply because it cannot state with particularity which piece of evidence will be found on which component of his system. [T]he prohibition of general searches cannot be confused with a demand for precise *ex ante* knowledge of the location and content of evidence related to the suspected violation. . . . Instead, the determination of the requisite particularity must be flexible and the description of items to be seized need only be as specific as the circumstances and the nature of the activity under investigation permit. The proper question is whether it was reasonable to provide a more specific description of the items at that point in the investigation. Defendant has provided no reason to expect the police to be able to identify which of the components of the home computer systems and media he used to accomplish the alleged crimes or to store evidence of them.

Id. at *6 (internal quotation marks and citations omitted).

That analysis applies here. The warrant for Defendant's house—in particular Addendum A—specifically lists types of media where evidence of or related to child pornography could be stored. Just because the list is long and may include all or nearly all of the devices in Defendant's home does not mean it is overbroad. The police could not have known ahead of time where evidence might be stored. And, as the warrant application described, evidence of child pornography can take many forms (e.g., images, videos, correspondence, computer logs, metadata, etc.) and be stored on a variety of devices (e.g., computers, tablets, phones, removable media, various storage devices, etc.). Given these circumstances, the warrant allowing the search and seizure of “[a]ny and all computers, ‘smart phones,’ ‘mobile data devices’ and ‘network’ equipment systems,” followed by

a list of examples of types of devices and systems, is particularized. *See id.* at *6 (“[T]he limitation in the warrant to seizure of components located in defendant’s home was as specific as the circumstances permitted.”) (internal quotation marks omitted).

2. Laptop Warrant

The analysis for the laptop warrant is similar to the analysis for the house warrant in that the police cannot know *ex ante* what types of digital evidence they will find and where on a computer they will find it. As the First Circuit has held, the police

cannot simply search certain folders or types of files for keywords. The same goes for other specific identifying information . . . This is because computer files are highly manipulable. A file can be mislabeled; its extension (a sort of suffix indicating the type of file) can be changed; it can actually be converted to a different filetype (just as a chat transcript can be captured as an image file, so can an image be inserted into a word-processing file and saved as such).

United States v. Farlow, 681 F.3d 15, 19 (1st Cir. 2012) (internal quotation marks and citations omitted).

Defendant takes issue with a list in the warrant application of certain files, data, and information about the use or ownership of the laptop and its contents but did not specifically identify which aspects of the list he believes are overbroad. The government countered with reasons why each category in that list is important and not broader than reasonably necessary. (Gov’t Opp. (Dkt. No. 67) at 7-8.) For example, information showing access, possession, control, use, or ownership of the laptop would answer the question of who was using the laptop, which is “as important as what was on the laptop.” (*Id.* at 7 (emphasis omitted).) And certain metadata and internet histories will show when files were created, accessed, or modified. (*Id.* at 7-8.)

Defendant is right that “the content of a computer file may not be obvious without opening the file itself.” (Mot. to Supp. Laptop Evidence (Dkt. No. 62) at 3.) While that could create an “incentive to seize more rather than less” (*Id.* (internal quotation marks and citation omitted)), there

is no indication that happened here. Instead, the fact that a file's contents may not be obvious without opening the file supports the government's argument that the scope of the warrant was reasonable because computer files are manipulable, and police could not have known *ex ante* how or where evidence would be stored in the laptop. This is underscored by the fact that Defendant felt comfortable giving the laptop to his neighbor to be fixed. Had Defendant believed child pornography would have been obvious or easy to find, it is doubtful he would have left the laptop with someone tasked with repairing it.

Before obtaining the laptop warrant, police could not have known how Defendant stored child pornography or evidence related to his possession or dissemination of child pornography with the precision Defendant demands. The portion of the warrant application regarding "internet history, user accounts, correspondence, etc." may be overbroad to the extent it includes "etc." But Defendant has not identified any evidence that was unlawfully searched because of the inclusion of "etc.," and the inclusion of "etc." does not render the warrant, as a whole, overbroad or unreasonable.¹

C. Even if the Warrants Are Overbroad, Suppression Is Not Warranted Because the Good Faith Exception Applies.

In the alternative, the government argues the good faith exception applies. The court need not reach that issue, but it agrees with the government. Even if the warrant were overbroad, suppression would be inappropriate because the warrants were not so deficient "as to render official belief in [their validity] entirely unreasonable." *United States v. Leon*, 468 U.S. 897, 923 (1984) (internal

¹ Partial suppression is appropriate when some evidence is seized due to infirm portions of a warrant and other evidence is seized under valid portions of a warrant. *See United States v. Morris*, 977 F.2d 677, 682 (1st Cir. 1992) ("[I]n cases where a search warrant is valid as to some items but not as to others, we have established that a court can admit the former while excluding the latter."); *United States v. Falon*, 959 F.2d 1143, 1149 (1st Cir. 1992) ("The remedy in the case of a seizure that casts its net too broadly is . . . not blanket suppression but partial suppression."). But Defendant has not argued for partial suppression or identified specific evidence that should be suppressed; he instead argues for blanket suppression, which, as explained above, is unwarranted.

quotation marks and citation omitted). The officers executing both warrants acted in good faith, and their reliance on them was objectively reasonable.

III. CONCLUSION

For the foregoing reasons, Defendant's motions to suppress (Dkt. Nos. 60 & 62) are DENIED.

/s/ Mark G. Mastroianni
MARK G. MASTROIANNI
UNITED STATES DISTRICT JUDGE